(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/77792 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/10498

(22) International Filing Date: 2 April 2001 (02.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/544,809 7 April 2000 (07.04.2000) US

(71) Applicant: **RSA SECURITY INC.** [US/US]; 36 Crosby Drive, Bedford, MA 01730 (US).

(72) Inventors: **JUELS, Ari**; 131 Freeman Street, Apt. 3, Brookline, MA 02446 (US). **WONG, Bonnie, M.**; 131 Freeman Street, Apt. 3, Brookline, MA 02446 (US).

(74) Agent: **FREEMAN, Kia, L.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/77792 A2

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A USER

(57) Abstract: The system and method provides for the authentication of a user based on graphical input provided by the user. The user enters graphical input, such as a squiggle, into a graphical interface. A verifier compares the input pattern to a secret input pattern to determine if the two patterns are approximately similar in order to authenticate the user. Typically, the verifier uses an approximation parameter to determine if the input and secret patterns are similar. Once the verifier authenticates the user, the user is allowed access to a resource, such as a computer system, portable computer, software application running on a computer system or other hardware device.

SYSTEM AND METHOD FOR AUTHENTICATING A USER

Field of the Invention

The invention relates generally to the field of security and authentication and, more particularly, to a system and method for using a graphic display to authenticate a user of a computer or other device.

Background of the Invention

Passwords have long been used to authenticate a user before providing access to a computer system or to some other device. They are easy to use and conceptually simple. They are probably the oldest and most common data security tool used in computing environments. Because they are generally alphanumeric in form and often closely related to words in natural language, passwords are relatively easy for users to remember. Typically, users can rapidly enter them through standard hardware peripherals such as keyboards. Nonetheless, in terms of their security properties, passwords have shortcomings. Typically, users derive their passwords from a limited portion of the lexicons in their native languages, making them easy to guess, particularly in automated computer attacks.

The vulnerability of passwords in computer systems is becoming increasingly problematic as computing and networking technologies aim to manage increasingly sensitive information. Consumers are beginning to use smart cards and other portable devices to carry digital cash. At the same time, corporations are making sensitive information more available on their networks and are employing digital signatures in committing to legally binding contracts. Hardware devices like smart cards and authentication tokens provide cryptographic authentication for such applications; but typically the cryptographic features of these devices are secured using passwords.

It is possible to broaden the distribution of passwords that are used in a system, and thereby strengthen the system by assigning randomly generated alphanumeric passwords to users. Even users with the most retentive memories, however, have difficulty remembering more than approximately seven alphanumeric characters. The total number of such seven character passwords is about $2^{35} \approx 10^{11}$, which is too small to provide resistance against an automated computer attack on the password. Strong resistance to automated password attacks requires a

password space on the order of about $2^{70} \approx 10^{21}$. This space corresponds to random, alphanumeric passwords of sixteen characters in length, which is too long for practical use by most users.

The difficulty users have in remembering enough password information to allow secure authentication is at odds with their ability to retain large amounts of other types of information in other contexts. A few examples of the other types of nonpassword data an individual may routinely remember are historical and personal events, the configuration of rooms in buildings, and the layout of city streets, not to mention the vocabulary and idioms of her native language. Some of that information may remain fixed in her memory over extended periods of time, even without frequent reinforcement.

A number of researchers have investigated the use of such everyday information in connection with mnemonic systems as a replacement for passwords. One authentication approach exploits the ability of users to recognize faces. To authenticate herself in this system, a user is asked to identify a set of familiar faces from among a gallery of photographs. While conveniently universal, this system has large memory requirements for the storage of the photographs, and has relatively slow data entry time. Another proposed approach is based on the use of routes on a complex subway system, such as the Tokyo subway system, in connection with secrets, suggesting that users could retain relatively large amounts of information in this context. This approach has the advantage of mnemonic naturalness, but has a strong disadvantage in its idiosyncrasy because not all users live in cities with subway systems or use a subway frequently.

A commercial system produced by Passlogix, Inc. of New York, New York effectively extends the mnemonic approach by allowing users to select from a range of mnemonic systems. Users can, for instance, choose to use an interface displaying a room containing a collection of valuables, and encode a password as a sequence of moves involving the hiding of these valuables in various locations around the room. This method of password entry appeals to a natural mnemonic device because it resembles the medieval system of the "memory palace," whereby scholars sought to archive data mentally in an imagined architectural space. By allowing the user to select a password herself, however, this approach is vulnerable to the problem of predictability that occurs with conventional password systems. Some passwords are more popular than others, since they are easier to remember. In one example, one-third of user-selected passwords could be found in the English dictionary. Similarly, in a mnemonic system, users are more likely to pick some sequences than others. In one example, a mnemonic system allows users to trade stocks; typically, the users will choose from among the most popular stocks, as these are the

easiest to remember. In seeking to guess a password in this system, an attacker is likely to gain a substantial advantage by choosing Dow Jones stocks. In principle, if user passwords are formed as sufficiently long random sequences of moves, a mnemonic system will provide an adequate level of cryptographic security. Typically, mnemonic systems are not designed to facilitate user memorization of random sequences, and may not even enforce a minimum sequence length in user password entry. A mnemonic system may also be cumbersome in terms of the user interaction involved in entering a password, in some cases demanding an involved sequence of non-uniform mouse movements to enter the password into a computer system.

Summary of the Invention

One objective of a system constructed according to the invention is to provide graphic or visual passwords that users can remember easily and for a long duration. Another objective is to provide a password that a user can enter with a minimum of physical effort, such as by minimal mouse movement or keystrokes, or by the use of a writing tool on a tool sensitive graphic display. An additional objective is that the entry of the password should require minimal mental effort.

Another objective of the invention is to provide flexible password entry. Unlike computer memory, human memory is prone to inaccuracy. One objective is to accommodate likely user errors.

Another objective of the invention is to provide a system adaptable to computing environments with limited memory, power, and graphical display capabilities. In addition, a system constructed according to the invention should be useable with a range of hardware peripherals, such as keyboards, mice, touch screens, and palmtop computer styluses.

In one aspect, the invention relates to a method for authenticating a user. The method includes determining a secret pattern, entering an input pattern from a user on a graphical interface, determining an approximation parameter that can be used to compare the secret pattern to the input pattern, comparing the secret pattern and the input pattern to determine if the secret pattern and the input pattern are approximately similar within limits defined by the approximation parameter, and authenticating the user based on the comparison.

In one embodiment, the method includes displaying a portion of the secret pattern on the graphical interface to the user. In another embodiment, the method includes determining the portion to display based on a display parameter.

In one embodiment, the method includes determining the secret pattern based on a grid. In another embodiment, the method includes selecting one or more blocks of cells in the grid based on the secret pattern. In another embodiment, the method includes comparing an input sequence for entering the input pattern with a secret sequence of the secret pattern.

In one embodiment, the method includes entering the input pattern on a displayed grid on the graphical interface. In another embodiment, the method includes entering a squiggle. In a further embodiment, the squiggle includes a random shape. In another embodiment, the method includes entering a symbol. In another embodiment, the method includes entering a sketch. In another embodiment, the method includes selecting one or more points on each of a plurality of images displayed on the graphical interface.

In another embodiment, the method includes allowing access to a resource in response to the step of authenticating the user.

In one embodiment, the method includes generating a calculated value of the secret pattern, generating a calculated value of the input pattern, and comparing the calculated value of the secret pattern and the calculated value of the input pattern. In another embodiment, the method includes generating a hash of the secret pattern and generating a hash of the input pattern.

In another embodiment, the method includes determining one or more secret points located in a display area and determining one or more approximation regions associated with one or more secret points.

In another embodiment, the method includes providing one or more memory cues to the user. In a further embodiment, the method includes providing one or more visual and/or auditory memory cues.

In another aspect, the invention relates to an authenticator for authenticating a user of a resource. The authenticator includes a graphical interface, a secret pattern, an input pattern, an approximation pattern, and a verifier. The graphical interface is capable of receiving graphical input from a user. The user enters the input pattern on the graphical interface. The approximation pattern can be used in comparing the secret pattern and the input pattern to determine if the secret pattern and the input pattern are approximately similar within limits defined by the approximation parameter. The verifier is in communication with the graphical interface and authenticates the user by comparing the secret pattern and the input pattern using the approximation parameter.

In one embodiment, the graphical interface displays a portion of the secret pattern to the user. In another embodiment, the graphical interface uses a display parameter to determine the displayed portion of the secret pattern.

In one embodiment, the secret pattern is based on a grid. In another embodiment, the approximation parameter includes one or more blocks of cells in the grid based on the secret pattern. In another embodiment, the input pattern includes an input sequence and the secret pattern includes a secret sequence, and the verifier compares the input sequence and the secret sequence.

In one embodiment, the graphical interface includes a displayed grid, and the user enters the input pattern on the displayed grid. In another embodiment, the input pattern includes a squiggle. In another embodiment, the squiggle includes a random shape. In another embodiment, the input pattern includes a symbol. In another embodiment, the input pattern includes a sketch.

In another embodiment, the user selects one or more points on each of a plurality of images displayed on the graphical interface when entering the input pattern on the graphical interface.

In another embodiment, the verifier allows access to a resource in response to authenticating the user.

In one embodiment, the verifier generates a calculated value of the secret pattern, generates a calculated value of the input pattern, and compares the calculated value of the secret pattern and the calculated value of the input pattern.

In another embodiment, the verifier generates a hash of the secret pattern and a hash of the input pattern.

In another embodiment, the graphical interface determines one or more secret points located in a display area and one or more approximation regions associated with one or more secret points.

In one embodiment, the graphical interface provides one or more memory cues to the user. In a further embodiment, the graphical interface provides one or more visual and/or memory cues.

Brief Descriptions of the Drawings

The invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description taken in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates a functional block diagram of an authenticator system based on graphical input according to one embodiment of the invention.

FIG. 2 illustrates a flowchart of the authentication process based on graphical input according to one embodiment of the invention.

FIG. 3 provides a pictorial view of a grid and secret graphical pattern of highlighted squares or cells according to one embodiment of the invention.

FIG. 4 provides a pictorial view of a grid and a secret pattern illustrated by connected line segments for one embodiment of the invention.

FIG. 5 provides a pictorial view of an input pattern that closely approximates the secret pattern illustrated in FIG. 4.

FIG. 6 provides a pictorial view of a partial display of the secret pattern illustrated in FIG. 4.

FIG. 7 provides a pictorial view of an approximation block of cells and an input pattern that is approximately similar to the secret pattern illustrated in FIG. 4.

FIG 8 provides a pictorial view of a display area, secret points located in the display area, approximation regions based on the secret points, and input points provided by a user, according to one embodiment of the invention.

Detailed Description of the Invention

FIG. 1 illustrates a functional block diagram of an authenticator system 110 including an input pattern 112, graphical interface 114, verifier 116, secret pattern 118, and approximation parameter 120. FIG. 1 also illustrates a user 124, who provides the input pattern 112 to the graphical interface 114, and a resource 126, which the verifier 116 allows the user 124 to access after verifying the input pattern 112 using the secret pattern 118 and the approximation parameter 120, as will be discussed in more detail later.

In one embodiment, the graphical interface 114 is a hardware device that provides a graphical display that can be viewed by the user 124 and which receives the input pattern 112 from the user 124. In another embodiment, the graphical interface 114 is a CRT (cathode ray

tube) with a touch screen capability. In another embodiment, the graphical interface 114 is a flat screen device, such as a LCD (liquid crystal display) or an active-matrix display device with input capability. In one embodiment, the graphical interface 114 is a separate device that is electronically, optically, or otherwise in communication with the verifier 116. In another embodiment, the graphical interface 114 is integrated into another device, such as a computer system, laptop computer, palmtop computer, other portable computer, or portable cellular telephone. In other embodiments, the other device also includes the verifier 116 and/or resource 126.

In one embodiment, the verifier 116 is a software application executing on a general purpose computer system. In alternate embodiments, the verifier 116 is implemented as a software module, program, or one or more objects, such as objects implemented in the C^{++} programming language. In another embodiment, the verifier 116 is a hardware device or integrated chip, such as an ASIC (application-specific integrated circuit).

In one embodiment, the resource 126 is a computer system, a database, or other resource that the user 124 desires to employ. In another embodiment, the resource 126 provides computational resources or data that the user 124 would like to access. In another embodiment, the resource 126 is a physical location or entity that the user 124 desires to access or use, such as a room, a locked automobile, or the locked ignition mechanism for an automobile.

In another embodiment, the graphical interface 114, verifier 116, and resource 126 are all part of the same computer system, laptop computer, palmtop computer, or other portable computer. In another embodiment, the graphical interface 114, verifier 116, and resource 126 are separate computers or devices connected in a network, which may be a local network, or a global network, such as the Internet.

In one embodiment, the authenticator system 110 uses tolerance parameters. In the embodiment of FIG. 1, two tolerance parameters are shown, an approximation parameter 120 and a display parameter 122. In this context, a tolerance parameter provides a tolerance or limit for how much information the user 124 is given or how accurate the user's 124 input must be. The approximation parameter 120 indicates how close the input pattern 112 must be to the secret pattern 118 for the verifier 116 to consider the input pattern 112 to be approximately similar to the secret pattern 118. The display parameter 122 indicates how much of the secret pattern 118 is displayed to the user 124. The user provides an input pattern 112 that matches the undisplayed portion of the secret pattern 118.

FIG. 2 illustrates a flowchart of the authentication process based on graphical input according to one embodiment of the invention. First, the verifier 116 determines a secret pattern 118 (step 200). In one embodiment, the verifier 116 determines a random pattern for the secret pattern 118. In another embodiment, the verifier 116 determines or calculates a pseudo-random pattern, or a secret pattern 118 based on a mathematical function. In other embodiments, the secret pattern 118 is provided to the verifier 116 from an external source, such as a database or a trusted authority, such as a server computer connected over a network to the verifier 116. The user receives or has access to the same secret pattern 118 or trusted authority.

Then the user 124 enters an input pattern 112 on the graphical interface 114 (step 202) in an attempt to match the secret pattern 118. In one embodiment, the user 124 is prompted with a portion of the secret pattern 118, which is displayed on the graphical interface 114 based on the display parameter 122. In one embodiment the display parameter 122 is a predetermined value obtained from a trusted authority, such as a server computer connected over a network to the graphical interface 114. In other embodiments, the graphical interface 114 or verifier 116 determines a random value for the display parameter 122 or uses a mathematical function to determine the display parameter 122.

Next, the verifier 116 determines an approximation parameter 120 (step 204). The verifier 116 uses the approximation parameter 120 to determine if the secret pattern 118 and input pattern 112 are approximately similar by comparing the secret pattern 118 and input pattern 112 (step 206). In one embodiment, the approximation parameter 120 is a predetermined value obtained from a trusted authority. In another embodiment, the verifier 116 determines the approximation parameter 120 using a mathematical function. In another embodiment, the approximation parameter 120 is determined before or concurrently with determining the display parameter 122. In one embodiment, the approximation pattern determines an approximation region 144 (see FIG. 8) that is circular, square, or some other shape.

In one embodiment, the verifier 116 compares the secret pattern 118 and input pattern 112 directly to verify that the two patterns are approximately similar. In another embodiment, the verifier 116 compares a calculated value for the secret pattern 118 with a calculated value for the input pattern 112.

In one embodiment, the verifier 116 compares a hash of the secret pattern 118 with a hash of the input pattern 112. In another embodiment the verifier 116 generates a hash of the secret

pattern 118 and stores this secret hash in a storage media, such as a hard disk, associated with the verifier 116 or authenticator system 110. In another embodiment, this verifier 116 stores the secret hash in a memory element, such as a ROM or RAM, associated with the verifier 116 or authenticator system 110. In another embodiment, the verifier 116 obtains the secret pattern 118 or secret hash over a network or secure channel. In a further embodiment, the verifier 116 compares a fuzzy or approximate value for the secret pattern 118 with a fuzzy or approximate value for the input pattern 112.

If the verifier 116 finds that the secret pattern 118 and the input pattern 112 are approximately similar, then the verifier 116 authenticates the user 124 (step 208) and allows the user 124 to access the resource 126.

FIG. 3 is a pictorial illustration of a grid 132 and a secret pattern 118 indicated by six highlighted squares or cells 13, 20, 26, 41, 49, and 63 in the grid 132. In one embodiment, the graphical interface 114 displays to the user 124 the grid 132, wherein each square or cell in the grid 132 has a different color or shade. In another embodiment the grid 132 also displays a recognizable image, such as a photograph. In other embodiments, the grid 132 is not square but is a rectangle or other geometric form or shape. In one embodiment, the grid 132 is a square matrix where each side of the grid 112 has k cells, and the matrix is referred to as a k by k grid 132.

In one embodiment, the secret pattern 118 consists of a randomly selected sequence $X = x_1, x_2, ..., x_n$ of n squares or cells in the grid 132 as illustrated by cells 13, 20, 26, 41, 49 and 63 in FIG. 3, where n has a value of 6. In another embodiment, the secret pattern 118 is a random squiggle that the user 124 must draw to within a certain tolerance, as described below. In other embodiments, the secret pattern 118 is a letter, number, or other symbol.

In the embodiment shown in FIG. 3, the grid 132 is a 10 by 8 matrix of 80 cells indicated by cell numbers 1 through 80. The use of a 10 by 8 matrix is exemplary only and is not a requirement of the invention. In other embodiments, grids 132 of other sizes or other geometric shapes may be used. In one embodiment, the user 124 provides an input pattern 112 by selecting the same points on the grid 132 in the same numerical sequence as the secret pattern 118, as indicated by the highlighted cells 13, 20, 26, 41, 49, and 63 in FIG. 3. In another embodiment, the secret pattern 118 includes a secret sequence indicating the order for entering the cells of the input pattern 112. For example, the required or secret sequence for the secret pattern 118 may be 26, 49, 63, 13, 41, and 20, and the user 124 must enter the same sequence as the input sequence

of the input pattern 112 on the graphical interface 114 before the verifier 116 determines that there is a match between the secret pattern 118 and the input pattern 112.

FIG. 4 is a pictorial illustration of a grid 132 and a secret pattern 118a. In FIG. 4 the secret pattern 118a includes cells 31, 22, 33, 43, 53, 64, 55, 56, 46, 47, 38, 48, 49, and 60. The secret pattern 118a shown in FIG. 4 is exemplary only. The secret pattern 118a is shown as a path extending generally from left to right, but this is not a requirement of the invention. Generally, the invention does not require a secret pattern 118 that tends in any one direction or forms any particular type of pattern. In alternate embodiments, the secret pattern 118 may be a random pattern, a pseudo-random pattern, or a pattern determined by a mathematical function. In FIG. 4 the secret pattern 118a is indicated by connecting lines. In other embodiments, the secret pattern 118a is indicated by curved lines, by a list of cell numbers, or other mechanism that indicates a unique secret pattern 118 in the grid 132.

FIG. 5 illustrates the grid 132 and the secret pattern 118a of FIG. 4 along with an input pattern 112a that a user 124 has entered that closely approximates the secret pattern 118a. The input pattern 112a touches the same cells in the grid 132 as the secret pattern 118a. In one embodiment, the verifier 116 determines that the input pattern 112a is approximately similar to the secret pattern 118a by determining that the two patterns 112a, 118a touch the same cells.

In one embodiment using a display parameter 122, the graphical interface 114 displays to the user 124 the first h squares in the sequence, $x_1, x_2, ..., x_h$ in a secret pattern 118. The value h is the display parameter 122 indicating that the graphical interface 114 displays only h squares of the secret pattern 118 to the user 124.

For example, FIG. 6 illustrates a displayed portion 134 of the secret pattern 118a of FIG. 4, for one embodiment of the invention. In this embodiment, h, the display parameter 122 has a value of 3, and the graphical interface 114 displays only the first three cells 31, 22, 33 of the secret pattern 118a. The user 124 must then enter an input pattern 112 that corresponds to the undisplayed portion of the secret pattern 118a. In other embodiments, the display parameter 122 may have values other than 3, and the displayed portion 134 may be based on cells other than the first cells of the secret pattern 118, such as cells in the middle of the pattern 118, cells at the end of the pattern 118 or a selected number of cells determined by other methods. In another embodiment, the graphical interface 114 displays to the user 124 cells from two or more separate portions of the secret pattern 118.

In one embodiment using the approximation parameter 120, the user 124 must select a square within an r×r block centered around x_{h+1}, then x_{h+2}, etc., through x_n to authenticate herself. The value r is the approximation parameter 120. The probability p that a guessed sequence X' is correct is easily seen to be $(r/k)^{2n-2k}$. Thus if $k = 100$, $r = 5$, $n = 10$, and $h = 2$, then $p \approx 10^{-19}$.

For example, in one embodiment, FIG. 7 illustrates the grid 132 with an approximation block 136 and an input pattern 112b that approximately matches the secret pattern 118a. In one embodiment, the approximation parameter 120 has a value of 3 and one cell of the input pattern 112b is considered a valid match if it is within a 3 by 3 approximation block 136 centered on a cell of the secret pattern 118a. The approximation block 136 illustrated in FIG. 7 is exemplary only, and an approximation block 136 may be centered or located at different cells on a secret pattern 118. For example, a 3 by 3 approximation block 136 centered on a central cell 22 of the secret pattern 118a includes cells 11, 12, 13, 21, 22, 23, 31, 32, and 33. Thus, in FIG. 7 cells 21 and 12 of the input pattern 112b do not match cells 31 and 22 of the secret pattern 118a, but the verifier 116 considers cells 21 and 12 to be close enough to the secret pattern 118a because they are within the approximation block 136 centered on cell 22. In general, in other embodiments, the approximation block 136 is adjusted for special conditions such as cells at the edges and corners of the grid 132. For example, the approximation block 136 may be enlarged or otherwise changed if the central cell of the block 136 is at the edge or corner of the grid 132. If a central cell, such as 31, is on the edge of the grid 132, then the 3 by 3 block 136 is adjusted appropriately. Thus the 3 by 3 block centered on cell 31 is set to a 2 by 3 block of the cells 21, 22, 31, 32, 41, and 42. In other embodiments, the approximation block 136 is adjusted in other ways, such as giving the approximation block 136 different sizes at different points in the secret pattern 112b. In general, the invention does not require the approximation block 136 to outline a square or rectangular shape, and, in other embodiments, the approximation block 136 outlines other geometric shapes.

FIG 8 illustrates a pictorial view of a display area 140, secret points 142a, 142b, 142c, 142d, 142e, referred to generally as 142, approximation regions 144a, 144b, 144c, 144d, 144e, referred to generally as 144, and input points 146a, 146b, 146c, 146d, 146e, referred to generally as 146, for one embodiment of the invention. The display area 140 is a visual area of the graphical interface 114 that the graphical interface 114 displays to a user 124. In other embodiments, the display area 140 is not a rectangle, as shown in FIG. 8, but is a square or other geometric form or shape.

The secret points 142a through 142e are part of a secret pattern 118 that is not displayed to the user 124 in one embodiment of the invention. The invention does not require that there be any specific number of secret points 142 such as the five secret points 142 shown in FIG. 8, and in other embodiments, other numbers of secret points 142 may be used in the secret pattern 118.

In another embodiment, the graphical interface 114 displays one or more points 142 of the secret pattern 118 on the display area 140 to the user 124 based on a display parameter 122. In one embodiment, the display parameter 122 indicates a value for the number of secret points 142 to be displayed. For example, if the display parameter 122 has a value of 2, then the graphical interface 114 displays two points, such as 142a and 142d, to the user 124. The invention does not require that the displayed secret points 142 be adjacent to each other or in any serial order. For a given display parameter 122 value, different secret points 142 may be selected to be displayed at different times.

In one embodiment, the graphical interface 114 displays an image or photograph that overlays the display area 140. If the graphical interface 114 displays an image or photograph, then in one embodiment the input points 146 are not displayed to the user 124. In another embodiment, the graphical interface 114 highlights or changes portions of the image corresponding to the locations of the input points 146. If a display parameter 122 is used, then the graphical interface 114 highlights portions of the image in the display area 140 that correspond to the one or more secret points 142 selected to be displayed based on the display parameter 122.

The input points 146 represent an input pattern 112 that the user 124 enters on the graphical interface 114. In one embodiment, the approximation regions 144 are regions within which the user 124 must make her selections of input points 146 for the verifier 116 to verify that the user 124 has entered a valid input pattern 112. Typically the approximation regions 144 are not displayed to the user 124. In FIG. 8 the input points 146 are represented by crosshairs or crossed lines, for one embodiment of the invention. In other embodiments, the input points 146 are represented by other geometric shapes, points, or symbols. In one embodiment, the user 124 must enter the input points 146 in a predetermined sequence, such as providing input points 142 to match a secret sequence of secret points 142a, 142c, 142e, 142b, and 142d. In another embodiment, the user 124 enters the input points 146 in any sequence.

In other embodiments, the approximations regions 144 are shapes other than the circles shown in FIG. 8. In other embodiments, the approximation regions 144 are of different sizes for different secret points 142.

In one embodiment, each input point 146 must be touching or within the approximation region 144. In another embodiment, one or more input points 146 are allowed to be outside the approximation regions 144 based on the approximation parameter 120, and the verifier 116 still determines that the input pattern and secret pattern 118 are approximately similar if most of the input points 146 are within the approximation regions 144. In another embodiment, the approximation parameter 120 determines the size of the approximation regions 144.

In one embodiment, the graphical interface 114 alters the shape of the approximation region 144 for one or more secret points 142. For example, if a secret point 142 is close to the edge of the display area 140, then part of the approximation region 144 for that secret point 142 is truncated by the boundary of the display area 140. The graphical interface 114 may alter the approximation region 144 in other ways. In one embodiment, the graphical interface 114 enlarges the approximation region 144 if it is close to the edge of the display area 140 or is partially truncated by the edge of the display area 140. In another embodiment, the graphical interface 114 determines only one approximation region, such as an ellipse or other shape, for two or more secret points 142 located close to each other.

In one embodiment, the secret points 142 are any points that can be determined in the display area 140. In another embodiment, the graphical interface 114 displays the display area 140 using pixels, and each secret point 142 is a pixel. In another embodiment, the approximation region 144 is based on a predetermined pixel-distance tolerance.

In one embodiment, the graphical interface 114 displays memory cues to the user 124 to encourage the user 124 to remember the secret pattern 118 so that the user 124 enters a valid input pattern 112 that the verifier 116 determines to be approximately similar to the secret pattern 118. The use of memory cues applies to displays based on grids 132 or display areas 140. The memory cues are either static or interactive. In addition, memory cues are either visual, auditory, or based on some other sensory medium accessible to the human senses.

In one embodiment, the graphical interface 114 provides a visual memory cue by changing the cursor shape or color depending on where on the graphical interface 114 the user 124 locates the cursor or stylus.

In another embodiment, the graphical interface 114 or the authenticator system 110 provides an auditory memory cue by playing a different piece of music for each image that the graphical interface 114 displays overlaying the grid 132 or the display area 140.

In another embodiment, the graphical interface 114 provides a visual memory cue by changing the color or brightness of the image, or of part of the image, displayed to the user 124 depending on where the user 124 locates the cursor or stylus on the graphical interface 114.

In one embodiment, the graphical interface 114 displays successive images to the user 124, wherein each image is determined dynamically based on the behavior and selections made by the user 124 when using a stylus or other input device to provide input to the graphical interface 114. In one embodiment, when the user 124 selects an input point 146 in a displayed image, the graphical interface 114 zooms in on the image or magnifies a portion of the image, which is then in turn displayed to the user 124. When the user 124 selects another input point 146, then the graphical interface 114 zooms in on the image again. The graphical interface 114 repeats this process until the user 124 has completed entering an input pattern 112.

In another embodiment, the graphical interface 114 displays a number of portals, such as doors, and the user 124 selects one of the portals. The graphical interface 114 then displays different images depending on which portal the user 124 selects. In one embodiment, the user 124 simulates entry through a door into another visual space, such as moving through one or more doors into one or more rooms in a building. In one embodiment, each door or portal represents a secret point 142 in the secret pattern 118. In another embodiment, each door or portal does not itself represent a secret point 142 in the secret pattern 118, but provides access to an image that includes one or more secret points 142.

In another embodiment, the graphical interface 114 displays other visual metaphors and schemas that a user 124 follows when moving through a visual space, such as moving along a road or a path, or traveling in a vehicle, automobile, space craft, or water borne ship. In other embodiments, the graphical interface 114 displays other visual spaces or metaphors, as is known in the arts of computer graphics, computer and electronic games, and virtual reality.

Having described the preferred embodiments of the invention, it will now become apparent to one of skill in the art that other embodiments incorporating the concepts may be used. It is felt, therefore, that these embodiments should not be limited to disclosed embodiments but rather should be limited only by the spirit and scope of the following claims.

CLAIMS

What is claimed is:

1. A method for authenticating a user, the steps comprising:

determining a secret pattern;

entering an input pattern from a user on a graphical interface;

determining an approximation parameter for use in comparing the secret pattern and the input pattern from the user;

comparing the secret pattern and the input pattern to determine if the secret pattern and the input pattern are approximately similar within limits defined by the approximation parameter; and

authenticating the user based on the comparing step.

2. The method of claim 1, further comprising a step of displaying a portion of the secret pattern on the graphical interface to the user.

3. The method of claim 2, wherein the step of displaying the portion of the secret pattern comprises determining the portion to display based on a display parameter.

4. The method of claim 1, wherein the step of determining the secret pattern comprises determining the secret pattern based on a grid.

5. The method of claim 4, wherein the step of determining the approximation parameter comprises selecting at least one block of cells in the grid based on the secret pattern.

6. The method of claim 1, wherein the step of comparing the input pattern and the secret pattern comprises comparing an input sequence for entering the input pattern with a secret sequence of the secret pattern.

7. The method of claim 1, wherein the step of entering the input pattern comprises entering the input pattern on a displayed grid on the graphical interface.

8. The method of claim 1, wherein the step of entering the input pattern comprises entering a squiggle.

9. The method of claim 8, wherein the squiggle comprises a random shape.

10. The method of claim 1, wherein the step of entering the input pattern comprises entering a symbol.

11 The method of claim 10, wherein the symbol comprises at least one of a letter and a number.

12. The method of claim 1, wherein the step of entering an input pattern comprises entering a sketch.

13. The method of claim 1, wherein the step of entering the input pattern further comprises selecting at least one point on each of a plurality of images displayed on the graphical interface.

14. The method of claim 1, further comprising a step of allowing access to a resource in response to the step of authenticating the user.

15. The method of claim 14, wherein the step of allowing access to the resource comprises allowing access to at least one of a hardware device, a computer system, a portable computer, a software application, and a database.

16. The method of claim 1, further comprising steps of generating a calculated value of the secret pattern and generating a calculated value of the input pattern; and wherein the step of comparing the secret pattern and the input pattern comprises comparing the calculated value of the secret pattern and the calculated value of the input pattern.

17. The method of claim 16, wherein the step of generating the calculated value of the secret pattern comprises generating a hash of the secret pattern and the step of generating the calculated value of the input pattern comprises generating a hash of the input pattern.

18. The method of claim 1, wherein the step of determining the secret pattern comprises determining at least one secret point located in a display area and determining at least one approximation region associated with the at least one secret point.

19. The method of claim 1, further comprising a step of providing at least one memory cue to the user.

20. The method of claim 19, wherein the step of providing at least one memory cue to the user comprises providing at least one of a visual memory cue and an auditory memory cue.

21. An authenticator for authenticating a user of a resource, comprising:

a graphical interface capable of receiving graphical input from a user;

a secret pattern;

an input pattern entered on the graphical interface by the user;

an approximation parameter for use in comparing the secret pattern and the input pattern to determine if the secret pattern and the input pattern are approximately similar within limits defined by the approximation parameter; and

a verifier in communication with the graphical interface, the verifier authenticating the user by comparing the secret pattern and input pattern using the approximation parameter.

22. The authenticator of claim 21, wherein the graphical interface displays a portion of the secret pattern to the user.

23. The authenticator of claim 22, wherein the graphical interface uses a display parameter to determine the displayed portion of the secret pattern.

24. The authenticator of claim 21, wherein the secret pattern is based on a grid.

25. The authenticator of claim 24, wherein the approximation parameter comprises at least one block of cells in the grid based on the secret pattern.

26. The authenticator of claim 21, wherein the input pattern comprises an input sequence and the secret pattern comprises a secret sequence, and the verifier compares the input sequence and the secret sequence.

27. The authenticator of claim 21, wherein the graphical interface comprises a displayed grid and the user enters the input pattern on the displayed grid.

28. The authenticator of claim 21, wherein the input pattern comprises a squiggle.

29. The authenticator of claim 28, wherein the squiggle comprises a random shape.

30. The authenticator of claim 21, wherein the input pattern comprises a symbol.

31. The authenticator of claim 30, wherein the symbol comprises at least one of a letter and a number.

32. The authenticator of claim 21, wherein the input pattern comprises a sketch.

33. The authenticator of claim 21 wherein the user selects at least one point on each of a plurality of images displayed on the graphical interface when entering the input pattern on the graphical interface.

34. The authenticator of claim 21, wherein the verifier allows access to a resource in response to authenticating the user.

35. The authenticator of claim 34, wherein the resource comprises at least one of a hardware device, a computer system, a portable computer, a software application, and a database.

36. The authenticator of claim 21, wherein the verifier generates a calculated value of the secret pattern and a calculated value of the input pattern; and compares the calculated value of the secret pattern and the calculated value of the input pattern.

37. The authenticator of claim 36, wherein the verifier generates a hash of the secret pattern and a hash of the input pattern.

38. The authenticator of claim 21, wherein the graphical interface determines at least one secret point located in a display area and at least one approximation region associated with the at least one secret point.

39. The authenticator of claim 21, wherein the graphical interface provides at least one memory cue to the user.

40. The authenticator of claim 39, wherein the graphical interface provides at least one of a visual memory cue and an auditory memory cue.

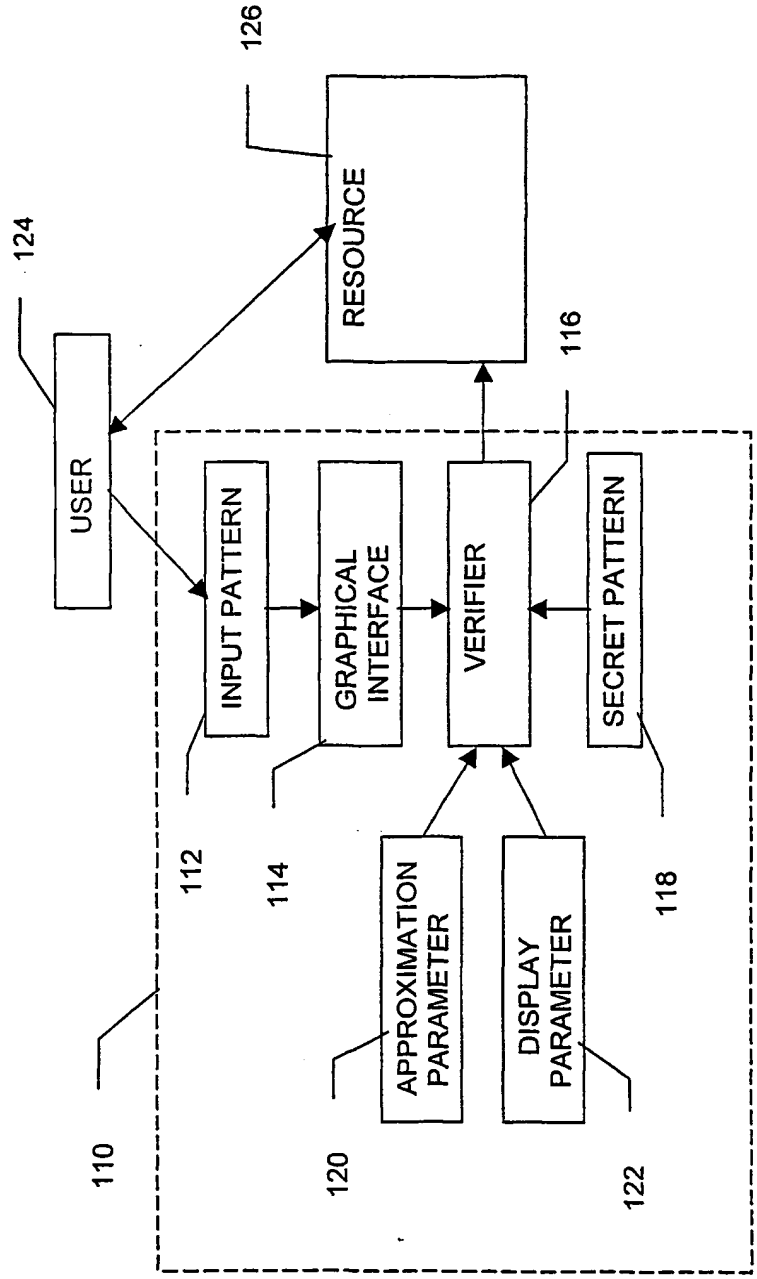

126
RESOURCE
124
USER
116
INPUT PATTERN
GRAPHICAL INTERFACE
VERIFIER
SECRET PATTERN
112
114
118
APPROXIMATION PARAMETER
DISPLAY PARAMETER
110
120
122

FIG. 1

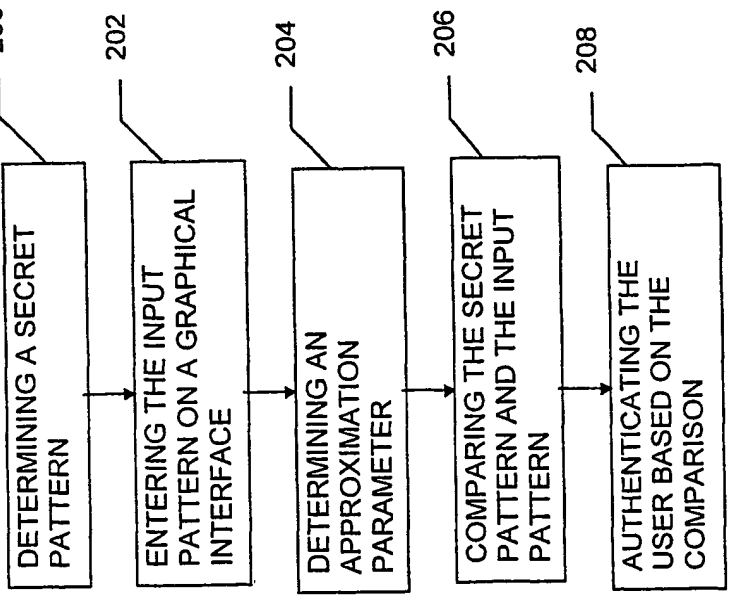


FIG. 2

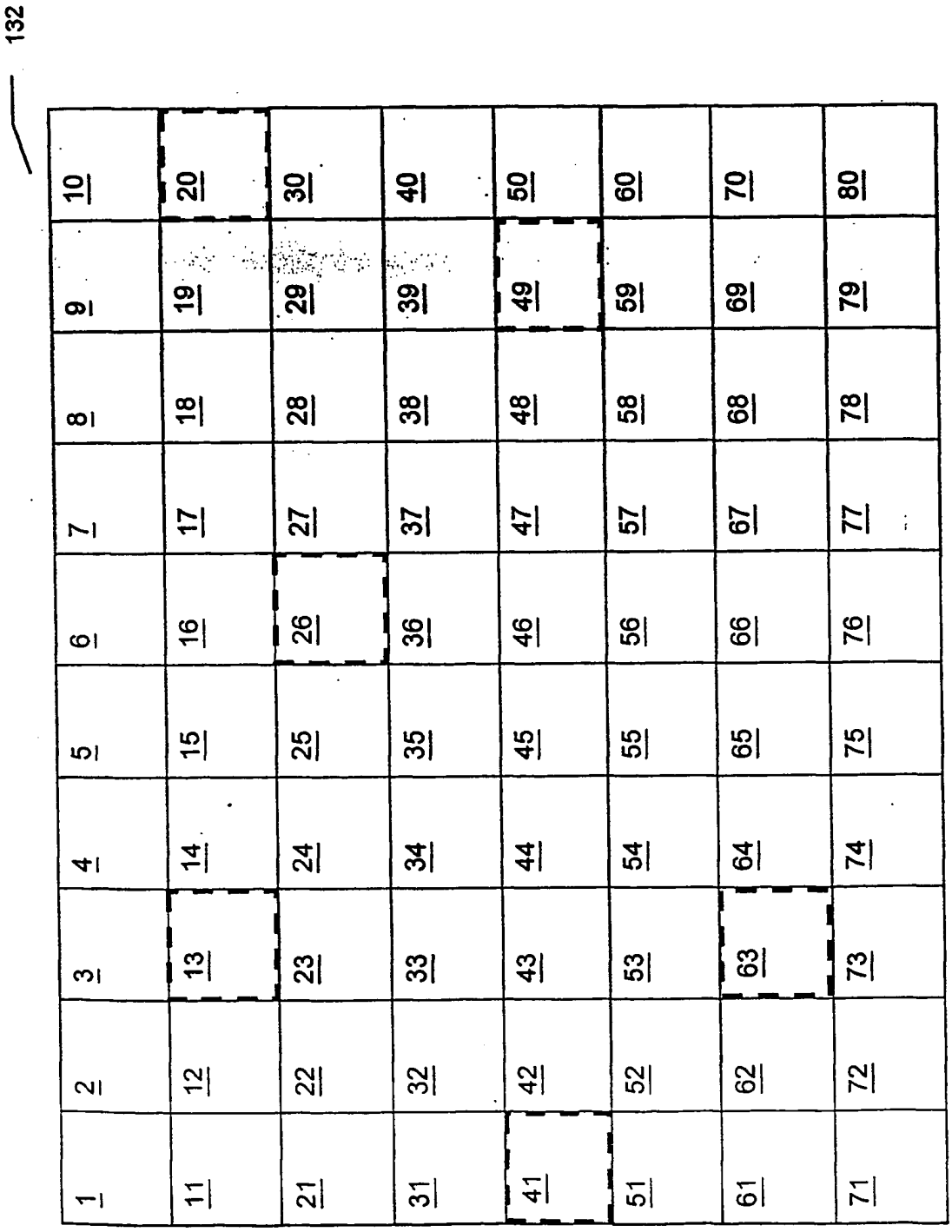

132
10 20 30 40 50 60 70 80
9 19 29 39 49 59 69 79
8 18 28 38 48 58 68 78
7 17 27 37 47 57 67 77
6 16 26 36 46 56 66 76
5 15 25 35 45 55 65 75
4 14 24 34 44 54 64 74
3 13 23 33 43 53 63 73
2 12 22 32 42 52 62 72
1 11 21 31 41 51 61 71

FIG. 3

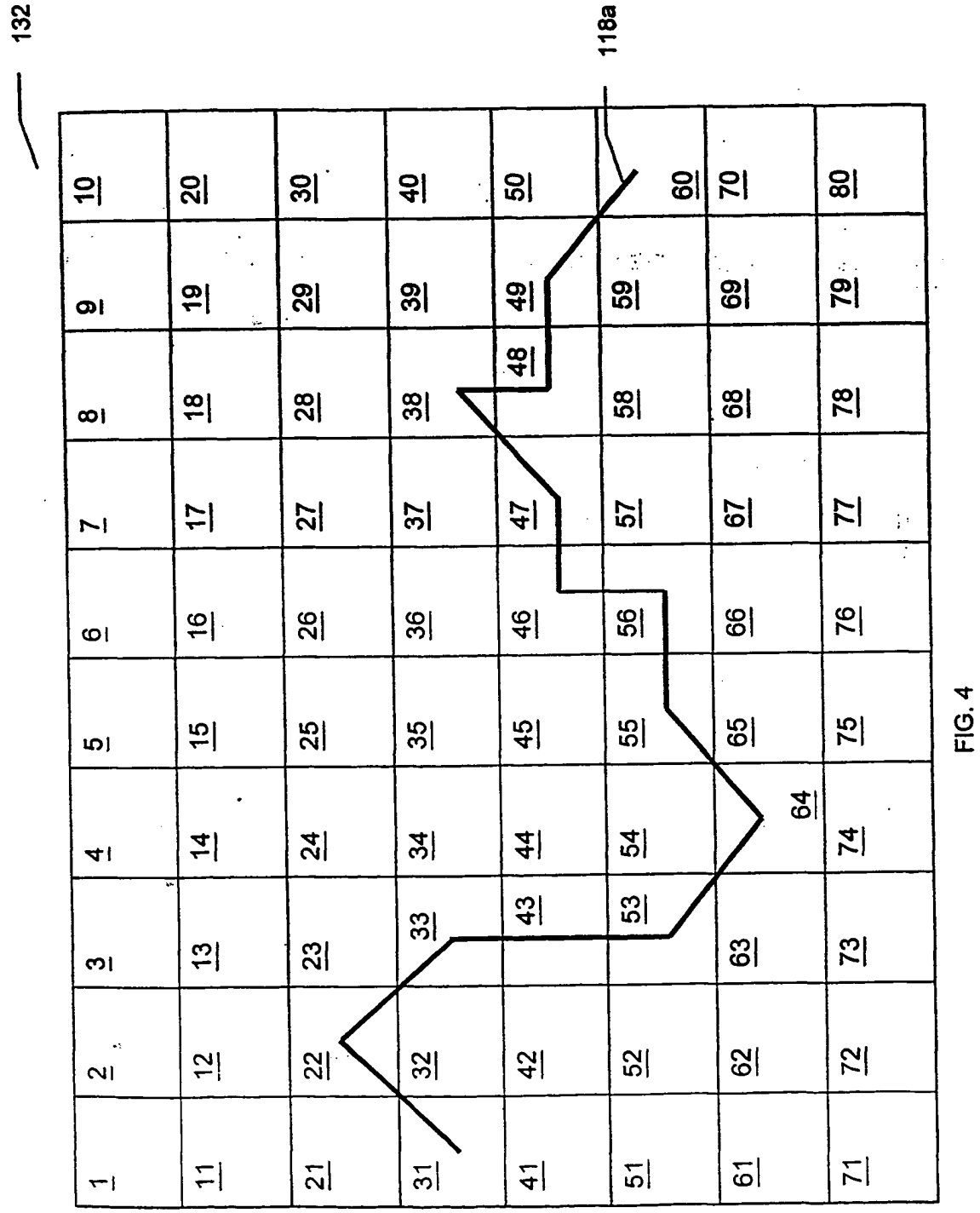

132
118a
1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50
51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70
71 72 73 74 75 76 77 78 79 80

FIG. 4

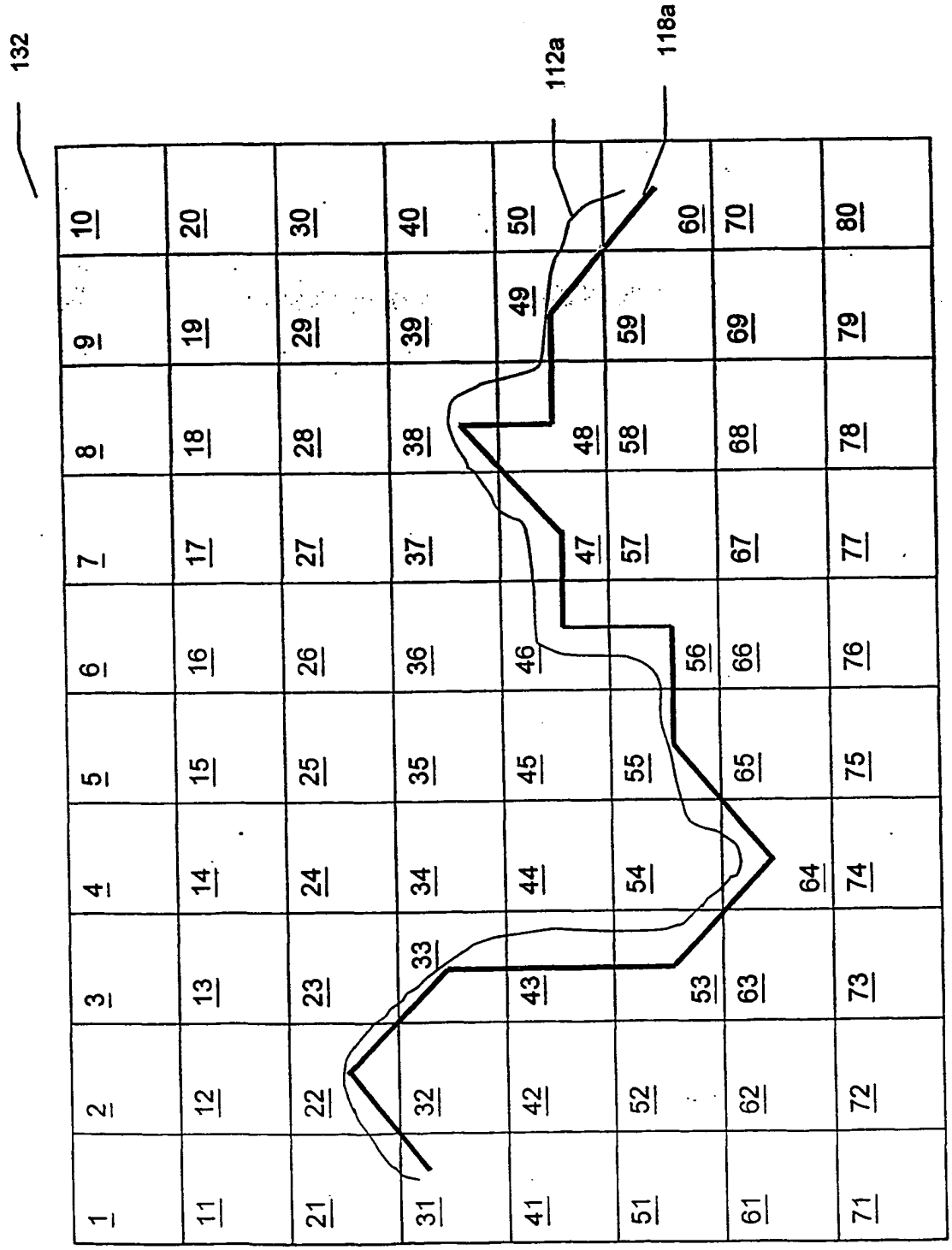

132
112a
118a
1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50
51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70
71 72 73 74 75 76 77 78 79 80

FIG. 5

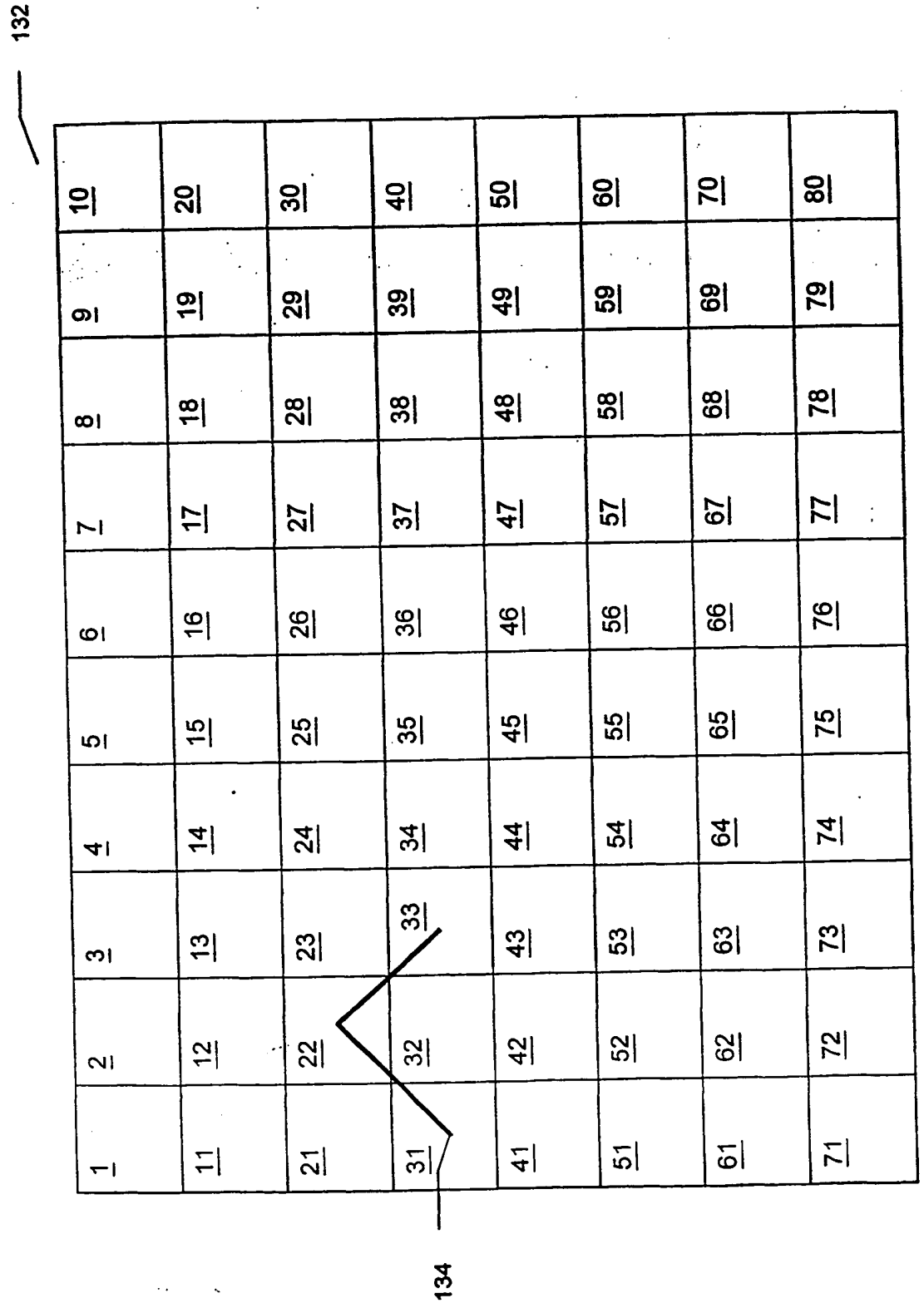


FIG. 6

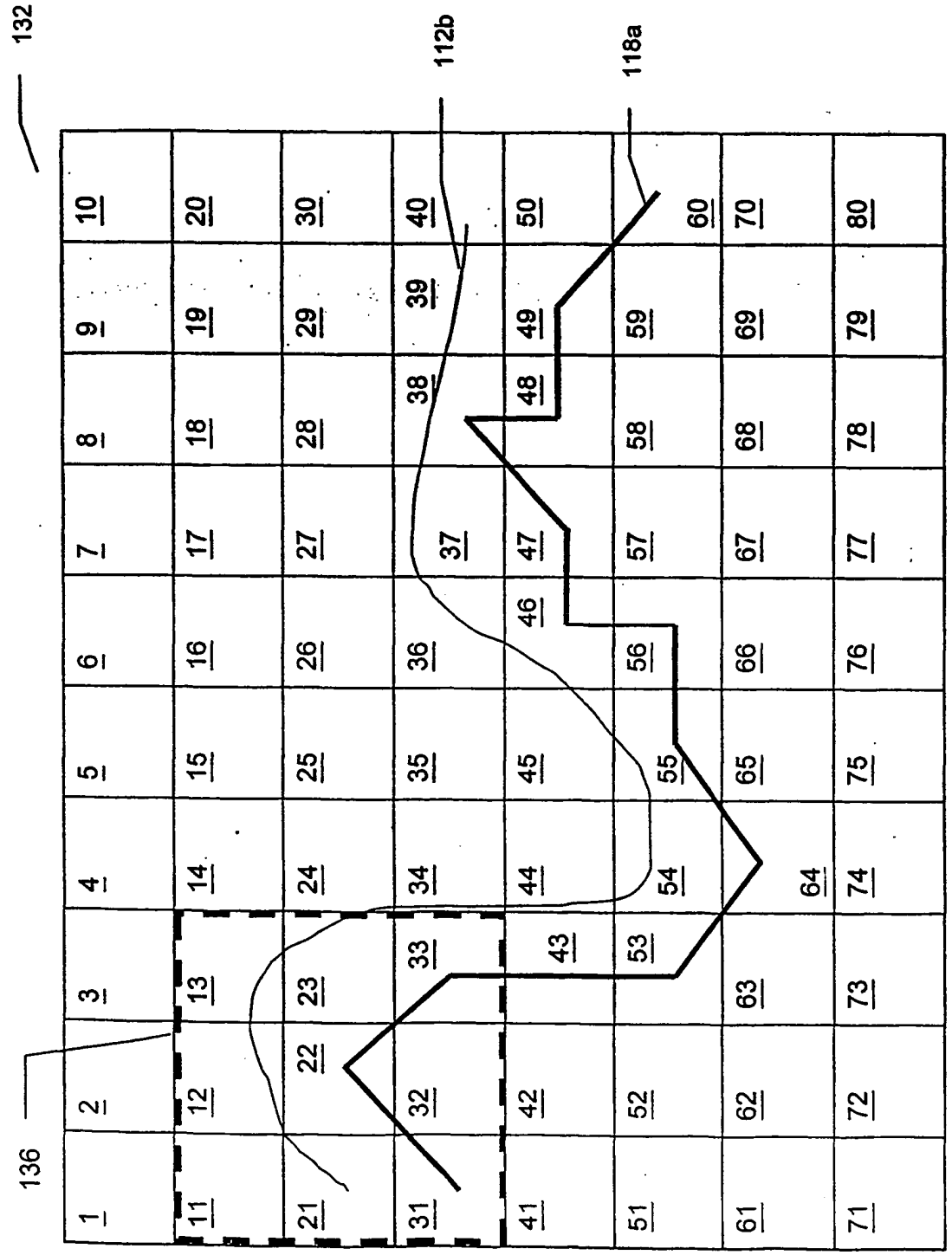

132
112b
118a
136
1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50
51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70
71 72 73 74 75 76 77 78 79 80

FIG. 7

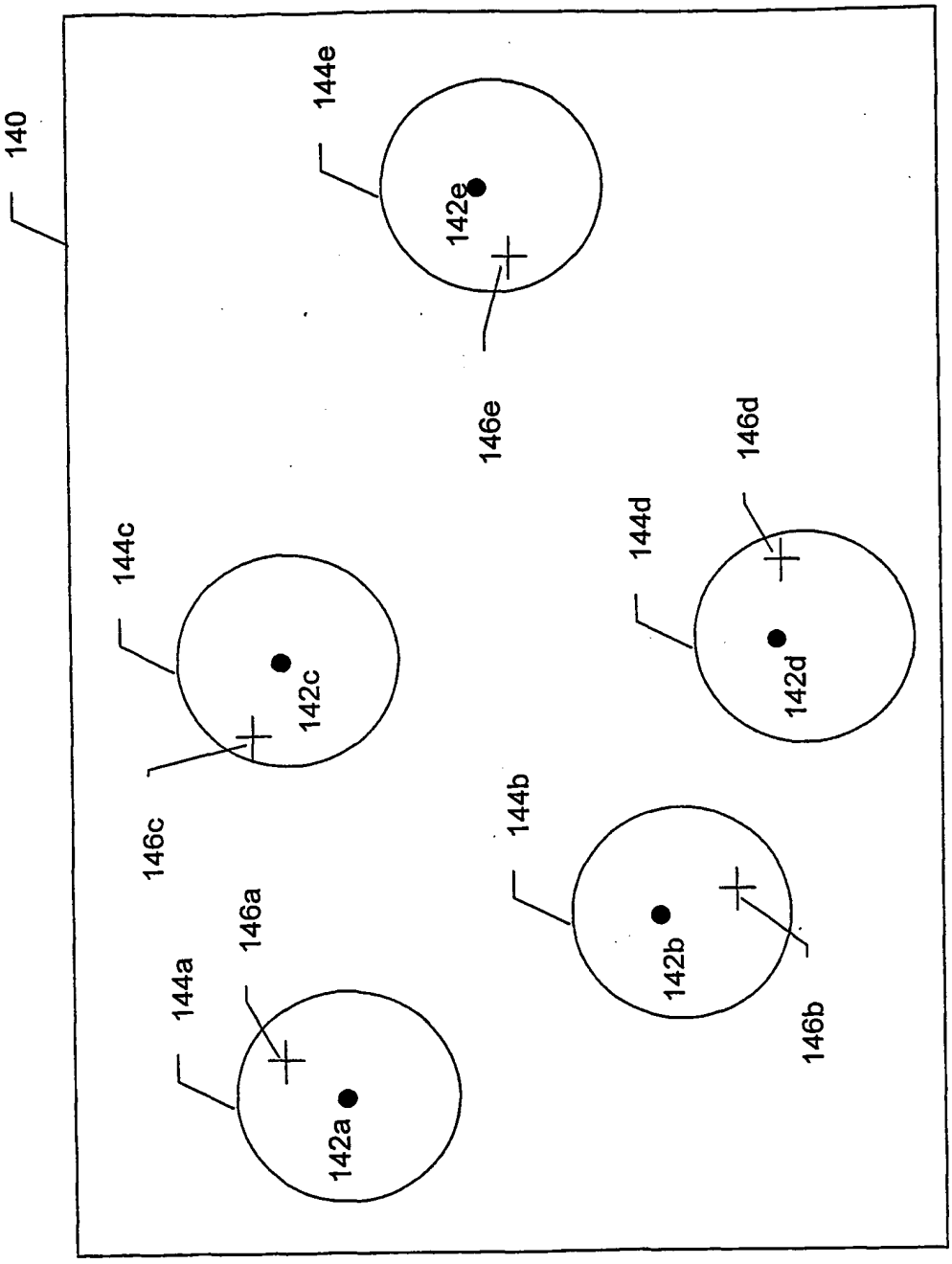


FIG. 8

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/077792 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/10498

(22) International Filing Date: 2 April 2001 (02.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/544,809 7 April 2000 (07.04.2000) US

(71) Applicant: **RSA SECURITY INC.** [US/US]; 36 Crosby Drive, Bedford, MA 01730 (US).

(72) Inventors: **JUELS, Ari**; 131 Freeman Street, Apt. 3, Brookline, MA 02446 (US). **WONG, Bonnie, M.**; 131 Freeman Street, Apt. 3, Brookline, MA 02446 (US).

(74) Agent: **FREEMAN, Kia, L.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

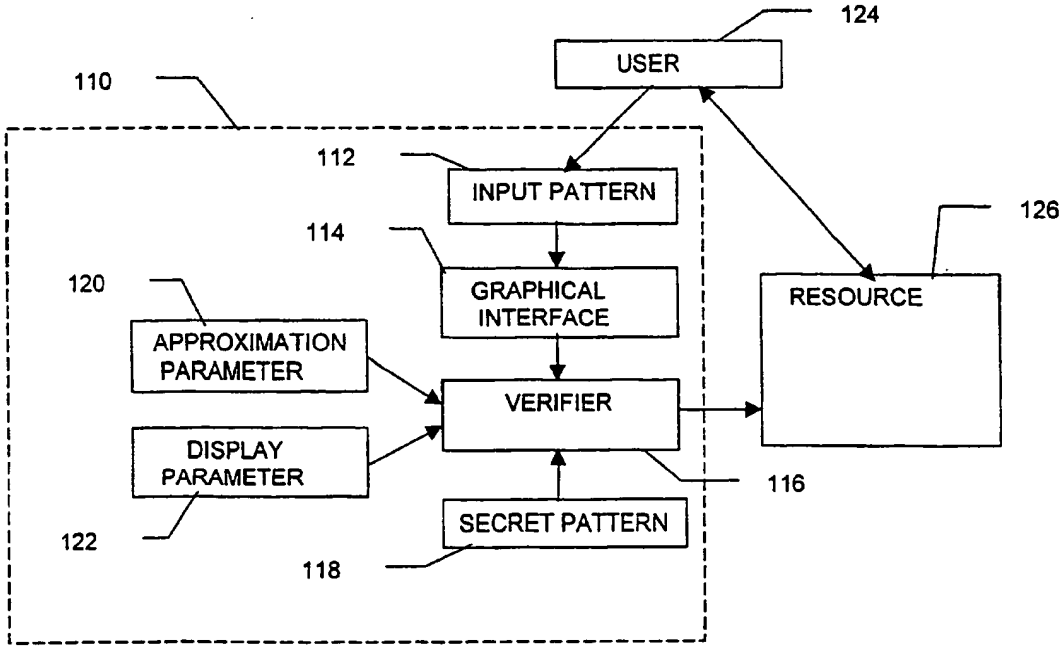
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
30 January 2003

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A USER



(57) Abstract: The system and method provides for the authentication of a user based on graphical input provided by the user. The user enters graphical input, such as a squiggle, into a graphical interface. A verifier compares the input pattern to a secret input pattern to determine if the two patterns are approximately similar in order to authenticate the user. Typically, the verifier uses an approximation parameter to determine if the input and secret patterns are similar. Once the verifier authenticates the user, the user is allowed access to a resource, such as a computer system, portable computer, software application running on a computer system or other hardware device.

WO 01/077792 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/10498

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 677 801 A (AT & T CORP) 18 October 1995 (1995-10-18) abstract; figures 2-4 column 1, line 46 - line 56 column 2, line 24 - line 34 column 4, line 8 - line 28 column 5, line 13 - line 18 column 6, line 14 - line 32	1-40
X	WO 99 21073 A (CASIO COMPUTER CO LTD ;SUZUKI HIDEO (JP)) 29 April 1999 (1999-04-29)	1,21
A	abstract; figures 1B,2	2-20, 22-40

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 August 2002	09/09/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kerschbaumer, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/US 01/10498

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 18139 A (PHILIPS ELECTRONICS NV ;PHILIPS NORDEN AB (SE)) 13 June 1996 (1996-06-13)	1,21
A	abstract; figure 6	2-20, 22-40
X	EP 0 901 060 A (FUJITSU LTD) 10 March 1999 (1999-03-10)	1,21
A	abstract; figures 11,16	2-20, 22-40
X	FR 2 765 979 A (RIVAILLER JACQUES) 15 January 1999 (1999-01-15)	1,21
A	abstract	2-20, 22-40

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Inte onal Application No
PCT/US 01/10498

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0677801	A	18-10-1995	EP	0677801 A1	18-10-1995
			JP	7295673 A	10-11-1995
			SG	24112 A1	10-02-1996
			US	5559961 A	24-09-1996
WO 9921073	A	29-04-1999	JP	11126191 A	11-05-1999
			AU	743522 B2	31-01-2002
			AU	9464298 A	10-05-1999
			CN	1271432 T	25-10-2000
			EP	1027639 A1	16-08-2000
			WO	9921073 A1	29-04-1999
			TW	406222 B	21-09-2000
WO 9618139	A	13-06-1996	WO	9618139 A1	13-06-1996
EP 0901060	A	10-03-1999	JP	11088324 A	30-03-1999
			EP	0901060 A2	10-03-1999
			US	6118872 A	12-09-2000
FR 2765979	A	15-01-1999	FR	2765979 A1	15-01-1999
			AU	8545998 A	08-02-1999
			EP	0995172 A1	26-04-2000
			WO	9903070 A1	21-01-1999

iSDOCID: <WO___0177792A3_I_>